MIT Bitcoin Expo, May 5, 2020

LONG TERM TRUST

AND

ANALOG COMPUTERS

Andrew Poelstra

Director, Blockstream Research

one

Hardware Wallets

Digital Hardware

What makes a safe hardware wallet?

- "not your keys, not your coins"; own the hardware
- trustworthy manufacturer
- the "genuine product" seal is unbroken

Digital Hardware

What makes a safe hardware wallet?

- secure element
- Bitcoin focused; supports PSBT, Taproot, etc
- simplicity? transparency?

Digital Hardware

What makes a safe hardware wallet?

- air-gapped
- pre-dates Bitcoin
- looks like a keyboard? printer? TI-85? gameboy?

Digital Hardware

What makes a safe hardware wallet?

- made out of paper and metal
- pre-dates the Reformation
- intermediate computations are literally incinerated

two

Trust and the Future

Failure Modes

How can you protect yourself?

- installing every software update?
- never installing software updates?
- updating hardware? stockpiling old hardware?
- never testing your backups? frequently testing your backups?

three

Trust and the Present

Failure Modes

How can a hardware wallet fail?

- generating bad keys
- signing without a PIN/button press
- directly leaking key material

Failure Modes

How can a hardware wallet fail?

- storage that won't erase
- signing things it shouldn't
- leaking key material via sidechannels

four

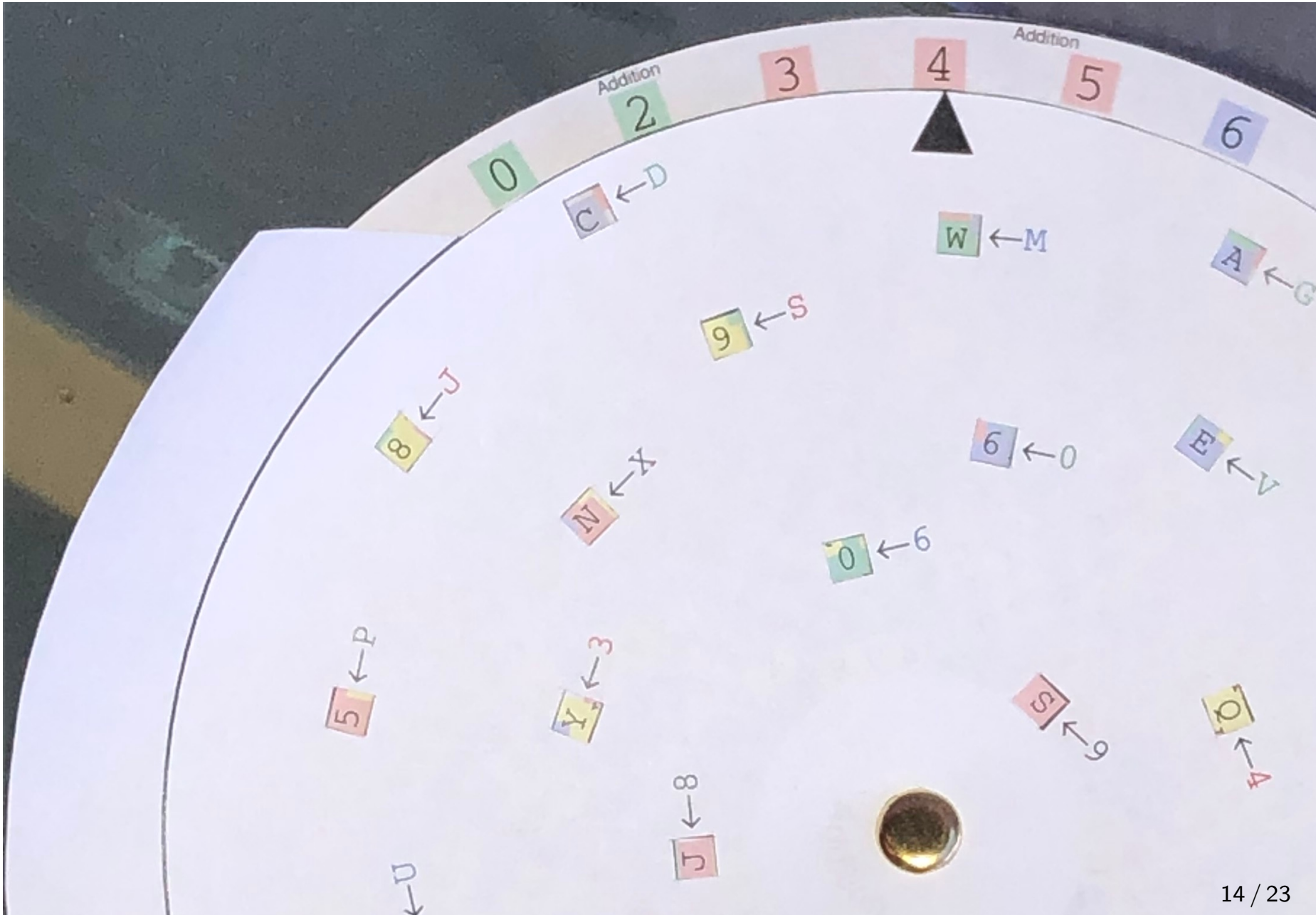
Volvelles (Trust the Past)

Volvelles

A **volvelle** is a paper computer made from two rotating discs

- Persia, 11th century (according to Wikipedia)
- used for early symmetric crypto (Alberti, 15th century)
- can implement finite field arithmetic (Galois, 19th century)
- such as polynomial interpolation (Lagrange, 18th century)
- this is Shamir's Secret Sharing! (Shamir, 20th century)

Volvelles


Addition
Addition
0
2
3
4
5
6
C ← D
W ← M
A ← G
9 ← S
8 ← J
6 ← 0
E ← V
N ← X
0 ← 6
5 ← P
Y ← 3
S ← 9
O ← A
J ← 8

Volvelles

Volvelles

And in those days there appeared in Alexandria a female philosopher, a pagan named Hypatia, and she was devoted at all times to magic, astrolabes and instruments of music, and she beguiled many people through (her) Satanic wiles.

– John, Bishop of Nikiu, from his *Chronicle* 84.87-103,
writing some 300 years later

Volvelles

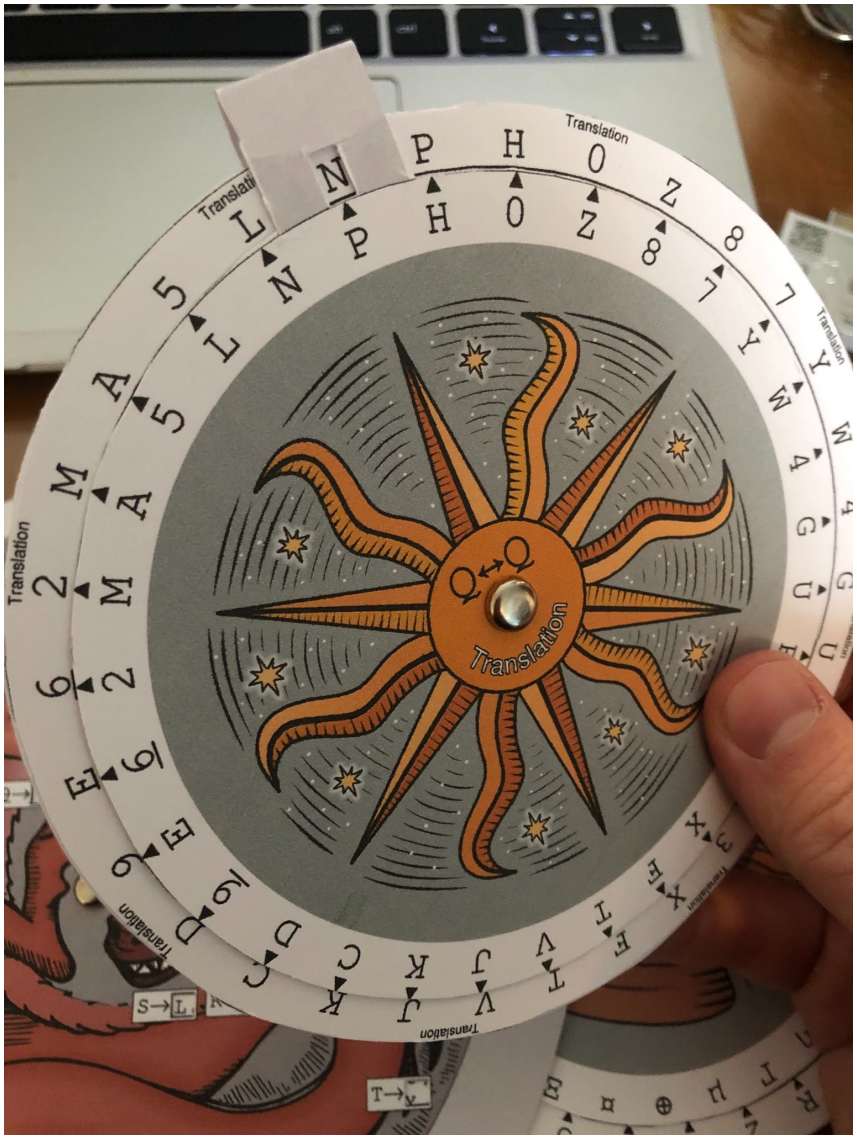
codex32 is a volvelle-based scheme that can

- generate random data (via de-biased dice)
- compute and verify checksums
- split and reconstruct secrets
- do symmetric encryption (via 2-of-2 secret sharing)

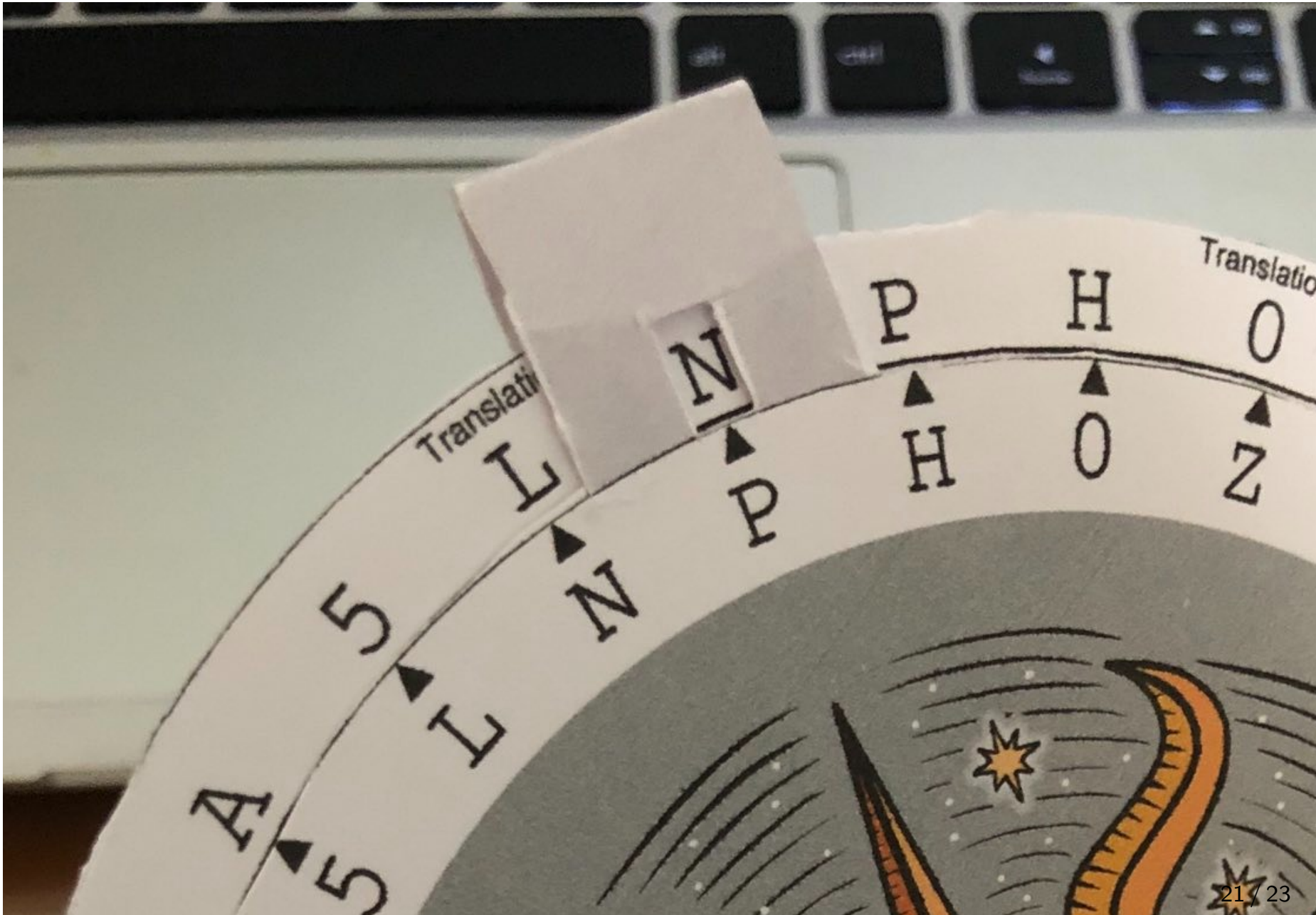
Volvelles

Volvelles

Volvelles


Translation
Translation
Translation
Translation
Translation
Translation

Volvelles



Volvelles

Benefits of paper:

- no EMF, microscopic storage, sidechannels
- understandable and verifiable without tools
- will continue to work, no matter how tech changes

`github.com/roconnor-blockstream/SSS32`

Volvelles by Leon Olsson Curr and Pearlwort Snead
Artwork by Michaela Paez (CC-BY)

`pearlwort@wpsoftware.net`